REMARKS

To date, the Examiner has not indicated that the subject matter of page 2 of the information disclosure statement (IDS) filed January 17, 2003 has been properly considered. A copy of such IDS is submitted herewith. If the Examiner requires additional copies of any reference(s), applicant invites the Examiner to contact the undersigned. Documentation in the file wrapper of the instant application confirming the Examiner's consideration of the relevant reference(s) is respectfully requested.

Claims 4-5 and 13-14 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant respectfully disagrees with such rejection, in view of the clarifications made hereinabove to the claims which overcome the same.

Claims 1-2, 4-11, and 13-20 again stand rejected under 35 U.S.C. §103(a) as being obvious over U.S. Patent No. 6,357,008, issued to Nachenberg ("Nachenberg"), and further in view of U.S. Patent No. 6,314,425, issued to Serbinis et al. ("Serbinis"). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove. Specifically, the subject matter of Claim 4 et al. has been incorporated into each of the independents claims.

In the latest action, the Examiner relies on the excerpts from Nachenberg below to meet applicant's claimed "server database engine comparing subsequently modified versions of the structured virus database to form a delta set of virus definition records, wherein the client database engine stores the delta virus definition records set into the structured virus database" (see this or similar, but not necessarily identical language in each of the independent claims).

> "Signature scanning antivirus programs work by scanning files for signatures of known viruses. A signature is a sequence of bytes that may be found in a virus program code, yet is unlikely to be found elsewhere. To "extract" a signature, an antivirus researcher must analyze the virus. Once this signature is determined, it is recorded in a database of virus signatures to be used by an antivirus program. The antivirus program scans a target program (executable file, boot record, or possibly document file with a macro) to detect the presence of a virus signature. If a signature is found, then the target program is deemed infected. Otherwise, the target program is considered uninfected." (col. 1, lines 27-33)

> "When the antivirus main module 151 is set to scan a target program (A, B, or C in FIG. 1) to determine heuristically whether or not the target program contains virus-like code, the main module 151 begins the decryption phase 252 which includes the following ten procedures 302, 304, 306, 308, 310, 312, 314, 316, 318, and 320." (col. 7, lines 25-27)

In reviewing the foregoing excerpts from Nachenberg (along with the remaining reference), it appears that the Examiner has not taken into consideration the full weight of applicant's claims. Specifically, as noted above, Nachenberg merely discloses the general concept of determining a signature as a result of an analysis by an antivirus researcher. This simply fails to rise to the level of specificity of applicant's claimed "server database engine comparing subsequently modified versions of the structured virus database to form a delta set of virus definition records, wherein the client database engine stores the delta virus definition records set into the structured virus database" (emphasis added), as claimed.

Still yet, the Examiner relies on col. 6, lines 27-53; and col. 8, lines 12-62 from Serbinis below to meet applicant's claimed "client database engine storing at least one updated virus definition record into the structured virus database indexed by the identifier and the at least one virus name for each virus definition record" (see this or similar, but not necessarily identical language in each of the independent claims). The Examiner continues by arguing that the relational database of Serbinis would allow indexing by identifiers and such is "inherent to a relational database."

While indexes may well indeed be inherent in relational databases, the content of applicant's claimed structured virus database and the manner in which applicant's claimed updated virus structured virus database is indexed would not be inherent in Serbinis. Specifically, Serbinis does not even suggest applicant's claimed "client database engine storing at least one updated virus definition record into the structured virus database indexed by the identifier **and** the at least one virus name for each virus definition record." (emphasis added), as claimed. Only applicant teaches and claims indexing updated virus definition records using both an identifier **and** the virus name for each virus definition record.

It appears that the Examiner has relied on an inherency argument regarding the above emphasized claim limitations. In view of the arguments made hereinabove, any such inherency argument has been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested. (See MPEP 2112)

Even still, the Examiner relies on the excerpts from Serbinis below to meet applicant's claimed "converter converting the virus definition records stored in the structured virus database into a virus data file comprising virus definition sets" (see this or similar, but not necessarily identical language in each of the independent claims).

> "The Originator then connects to the Internet using his or her web browser and enters the URL for the DMS system. Once connected to the DMS system website, at step 81, the Originator initiates a user session with DMS system 17 using a logon process, described hereinbelow.
>
> The Originator then fills out appropriate forms indicating a desire to upload the previously created electronic document to the DMS system, and at step 82 defines a list of Authorized Users who may access the document. The Originator specifies the types of access that each Authorized User is to receive, and metadata concerning the

> document (e.g., expiration date, etc.). Thus, for example, some Authorized Users may be granted access only to retrieve and review a document, while others are granted access to retrieve and modify the document. The specific access rights granted to each Authorized User are recorded in the document tables of DMS database 25, and the transaction is logged in the transaction tables of DMS database 25.
>
> At step 83, the Originator requests that the document be uploaded and stored in store 30 of the DMS system. Appropriate records are generated in the document tables of DMS database 25, and the transaction is logged in the transaction tables of DMS database 25. At step 85, the document is uploaded, for example, using HTTP or FTP, and stored in store 30. During the upload process, at step 84, the document optionally may be automatically or selectively filtered in accordance with routines appropriate for the service being performed. For example, the document may be automatically compressed or encrypted, or at the Originator's request, converted to a particular file format suitable for the Authorized Users (e.g., converted from WordPerfect.RTM. to Microsoft Word). Other forms of filtering may include formatting, translating or virus checking. Both the storage and filtering step, if performed, are logged to the appropriate tables in DMS database 25.
>
> At step 86, notification server 35 generates notification messages to the Authorized Users informing those Users that the document is available in store 30. The notification server also may provide a notification to the Originator that the notifications to the Authorized Users have been sent or delivered, as described hereinbelow with respect to FIGS. 12A and 12B. Issuance of any notifications to the Originator and Authorized Users are logged in the Notification tables and Transaction tables of DMS database 25. At any time after the document has been stored to store 30 at step 83, the Originator may terminate his or her user session." (col. 10, lines 15-61)

In reviewing the foregoing excerpt from Serbinis (along with the remaining reference), it appears that the Examiner has again not taken into consideration the full weight of applicant's claims. Specifically, as noted above, Serbinis merely discloses converting a document to a particular file format suitable for the Authorized Users (e.g., converted from WordPerfect.RTM. to Microsoft Word). This simply fails to rise to the level of specificity of applicant's claimed "converter converting the virus definition records stored in the structured virus database into a virus data file comprising virus definition sets" (emphasis added), as claimed.

It appears that there are many additional claim limitations not fully considered by the Examiner. As yet another example, note at least the emphasized limitations below:

> "each virus definition set comprising:
>
> binary data encoding instructions to detect the computer virus within a computer system, wherein the instructions comprise the object code to detect the identified computer virus;
>
> binary data encoding instructions to clean the computer virus from the computer system, wherein the instructions comprise the object code to clean the identified computer virus; and
>
> names associated with the computer virus" (emphasis added).

Only applicant teaches and claims a virus definition set with such specific binary data encoding and other related contents.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima* *facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, the subject matter of Claim 4 et al. has been incorporated into each of the independents claims.

With respect to the subject matter of former Claim 4 et al. (now at least substantially incorporated into each of the independent claims), the Examiner, in a blanket manner, relies on the following excerpts below from Nachenberg to meet applicant's claimed "server database engine [that] builds the virus definition records into the structured virus database by generating the identifier for each virus definition record and populating each virus definition record with the virus definition sentence and the virus removal sentence for the computer virus" (see this or similar, but not necessarily identical language in each of the independent claims).

> "A signature scanning antivirus program can identify particular virus strains for removal and may have a low "false-positive" rate if properly implemented. However, only viruses whose signatures have already been determined and stored in the signature database may be detected using signature scanning. Moreover, the signature database must be updated frequently to detect the latest viruses." (col. 1, lines 39-45)

The Examiner continues by arguing that applicant's claim limitations are inherent in the foregoing teaching. Again, it appears that the Examiner has not taken into consideration the full weight of applicant's claims. Specifically, the foregoing excerpt simply discloses a "signature database." This clearly falls short of applicant's claimed "server database engine [that] **builds** the virus definition records into the structured virus database by generating the identifier for each virus definition record and populating each virus definition record with the virus definition sentence and the virus removal sentence for the computer virus" (emphasis added), as claimed.

Again, it appears that the Examiner has relied on an inherency argument regarding the above emphasized claim limitations. In view of the arguments made hereinabove, any such inherency argument has been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested. (See MPEP 2112)

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claims 2 and 6, the Examiner has relied on the col. 2, lines 18-25 and col. 1, lines 39-45 from Nachenberg to make a prior art showing of applicant's claimed "anti-virus language decompiler converting each virus definition set in the virus data file into a virus definition record." There is simply no decompiler taught by Nachenberg, let along one for "converting each virus definition set in the virus data file into a virus definition record," as claimed. In view of such, any inherency argument has been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested. (See MPEP 2112)

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The

Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P376/00.140.01).

Respectfully submitted,

By: ______________________
Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

Telephone: (408) 971-2573
Facsimile: (408) 971-4660